U.S. DEPARTMENT OF COMMERCE PATENT & TRADEMARK OFFICE

B/O Form PTO-1390 **Transmittal Letter to the United States Designated/Elected Office (DO/EO/US) Concerning a Filing Under *35 USC 371***		*Attorney's Docket Number* RICH3001/JEK
		U.S. Application Number (if known) 09/926460
International Application Number PCT/EP00/04141	*International Filing Date* 09 May 2000	*Priority Date Claimed* 10 May 1999
Title of Invention DEVICE FOR PROTECTING THE INITIAL UTILIZATION OF A PROCESSOR/CHIP CARD		
Applicant(s) for DO/EO/US Oliver RICHTER	Assignee	

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items under *35 USC 371*:

1. ☒ This is a **FIRST** submission of items concerning a filing under *35 USC 371*.

2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under *35 USC 371*.

3. ☒ This express request to begin national examination procedures *(35 USC 371(f))* at any time rather than delay examination until the expiration of the applicable time limit set in *35 USC 371(b)* and PCT Articles 22 and 39(1).

4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.

5. ☒ A copy of the International Application as filed *35 USC 371(c)(2)*.
   a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☒ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).

6. ☒ A translation of the International Application into English *(35 USC 371(c)(2))*.

7. ☒ Amendments to the claims of the International Application under PCT Article 19 *(35 USC 371(c)(3))*
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.

8. ☐ A translation of the amendments to the claims under PCT Article 19 *(35 USC 371(c)(3))*.

9. ☒ An oath or declaration of the inventor(s) *(35 USC 371(c)(4))*. (☐ Executed ☒ Unexecuted)

10. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 *(35 USC 371(c)(5))*.

Items 11 to 16 below concern other document(s) or information included:

11. ☐ An Information Disclosure Statement under *37 CFR 1.97* and *1.98*.

12. ☐ An assignment document for recording. A separate cover sheet in compliance with *37 CFR 3.28* and *3.31* is included.

13. ☒ A **FIRST** preliminary amendment.
    ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.

14. ☐ A substitute specification.

15. ☐ A change of power of attorney and/or address letter.

16. ☒ Other items or information: 1 sheet formal drawing

Application Number (if Known)	International Application Number	Attorney's Docket Number
09/926460	PCT/EP00/04141	RICH3001/JEK

	Calculations	PTO USE ONLY
17. The following fees are submitted: **Basic National Fee** ***(37 CFR 1.492(a)(1)-(5)):*** ☒ Search report has been prepared by the EPO or JPO . . . . . $890.00 ☐ International Preliminary Examination Fee paid to USPTO *(37 CFR 1.482)* . . . . . $710.00 ☐ No International Preliminary Examination Fee paid to USPTO *(37 CFR 1.482)* but International Search Fee paid to USPTO *(37 CFR 1.445(a)(2))* . . . . . $740.00 ☐ Neither International Preliminary Examination Fee *(37 CFR 1.482)* nor International Search Fee *(37 CFR 1.445(a)(2))* paid to USPTO . . . . . $1040.00 ☐ International Preliminary Examination Fee paid to USPTO *(37 CFR 1.482)* and all claims satisfied provisions of PCT Article 33(1)-(4) $100.00		
ENTER APPROPRIATE BASIC FEE AMOUNT	**$ 890.00**	
Surcharge of **$130.00** for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date *(37 CFR 1.492(e))*.		

CLAIMS	NUMBER FILED		NUMBER EXTRA	RATE		
Total Claims	11	-20 =		× $18.00		
Independent Claims	2	-3 =		× $84.00		
Multiple Dependent Claims (if applicable)				+ $280.00	$ 280.00	
TOTAL OF ABOVE CALCULATIONS					**$ 1,170.00**	
Reduction by ½ for filing by small entity, if applicable. Small Entity Status is asserted pursuant to 37 CFR 1.27 for this application.						
SUBTOTAL					**$ 1,170.00**	
Processing fee of **$130.00** for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date *(37 CFR 1.492(f))*.						
TOTAL NATIONAL FEE					**$ 1,170.00**	
Fee for recording the enclosed assignment *(37 CFR 1.21(h))*. The assignment must be accompanied by an appropriate cover sheet *(37 CFR 3.28, 3.31)*. **$40.00** per property.						
TOTAL FEES ENCLOSED					**$ 1,170.00**	
Amount to be:					Refunded:	
					Charged:	

a. ☒ A check in the amount of **$1,170.00** to cover the fees is enclosed.

b. ☐ Please charge my **Deposit Account Number 02-0200** in the amount of $ _____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to **Deposit Account Number 02-0200**. A duplicate copy of this sheet is enclosed.

Note: Where an appropriate time limit under *37 CFR 1.494* or *1.495* has not been met, a petition to revive *(37 CFR 1.137(a) or (b))* must be filed and granted to restore the application to pending status.

Customer 23364

BACON & THOMAS, PLLC
625 SLATERS LANE - FOURTH FLOOR
ALEXANDRIA, VIRGINIA 223124-1176
(703) 683-0500

DATE: 07 November 2001

Respectfully submitted,

J. Ernest Kenney

J. Ernest Kenney
Attorney for Applicant
Registration Number: 19,179

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

International Patent Application No. PCT/EP00/04141

PCT/DO/EO/US

International Filing Date: 09 May 2000

Attorney Docket: RICH3001/JEK

Applicant: Oliver RICHTER

For: DEVICE FOR PROTECTING THE INITIAL UTILIZATION OF A PROCESSOR/CHIP CARD

PRELIMINARY AMENDMENT

Commissioner for Patents
Washington, D.C. 20231

Sir:

This paper accompanies documents submitted to establish the U.S. national stage of the above-identified international patent application under 35 U.S.C. §371.

The claims were not amended during the international phase. Before calculation of the filing fee and before examination, please amend the application as follows:

IN THE CLAIMS:

Please amend the claims 1 - 9 as shown on the appended APPENDIX OF CLAIMS. Also appended hereto an APPENDIX OF MARKED UP CLAIMS showing the changes which have been made.

REMARKS

All rights are reserved to the original claimed subject matter. The claims have been amended to reduce the filing fees and to better conform to U.S. claim format. Examination of the application as amended is respectfully requested.

Respectfully submitted,
BACON & THOMAS, PLLC

J. Ernest Kenney

J. ERNEST KENNEY
Attorney for Applicant
Registration No. 19,179

Customer 23364

BACON & THOMAS, PLLC
625 Slaters Lane - 4th Floor
Alexandria, VA 22314-1176
Telephone: (703) 683-0500
Facsimile: (703) 683-1080

Date: November 6, 2001

S:\Producer\jek\RICHTER - RICH3001\preliminary amendment wpd

APPENDIX OF CLAIMS

1(Amended). A method for putting into operation a processor smart card for a network for communication, for example a GSM network, wherein the card user must identify himself with respect to the processor smart card (SIM) by a personal identification number, comprising the steps:

- for execution control of the first use, the processor smart card is first provided by the card manufacturer or card personalizer with an additional application, preferably using the SIM Application Toolkit, which prevents its use in the network, instead allowing only local use by means of a card reader or card terminal, preferably a mobile phone device, and

- upon the first use of the processor smart card, the application outputs without a further check of a secret number a display signal for the first use and a request for confirmation, and

- after receiving a confirmation signal the additional application is deactivated or its execution so changed that upon the next use of the card a display signal is outputted to indicate that the card has already been put into operation and the use of the processor smart card in the network is enabled.

2(Amended). The method according to claim 1, wherein a personal identification number previously defined, preferably by the card manufacturer or card personalizer, must be inputted for activating the additional application.

3(Amended). The method according to claim 1 or 2, wherein the entry of a personal identification number (PIN) and/or a secret number (PUK) for changing or unblocking the personal identification number (PIN) is requested after the first use of the card and prior to the deactivation or change of state of the additional application.

4(Amended). The method according to any of claims 1 or 2, wherein some or all personal identification numbers on the card were already personalized on the processor smart card by the card manufacturer and said numbers are indicated upon the first use for later use on the card reader or card terminal, preferably a mobile phone device.

5(Amended). The method according to claim 1, wherein some or all personal identification numbers on the card are set by a random-number generator built into the card and said numbers are indicated during the first use on the card reader or card terminal, preferably a mobile phone device.

6(Amended). The method according to claim 1, wherein some or all personal identification numbers are combined for transmission to the network, preferably in encrypted form via a data channel, and sent immediately or at a later time to a central place at the network operator or network service provider.

7(Amended). The method according to claim 1, wherein the secret numbers to be defined at the first putting into operation are used not for the purpose of protecting the network application but for protecting an additional application, preferably a SIM Application Toolkit application, on the SIM card.

8(Amended). The method according to claim 1, wherein information, on the first use of the processor smart card and on the personal identification numbers is outputted or inputted via the hearing or speaking devices of the card reader, the card terminal or preferably the mobile phone device.

9(Amended). A smart card comprising a microprocessor (μP), a memory area (M) and an interface (*S*) each connected with the microprocessor (μP), and further comprising a memory area (*A*) where an application for the execution control of the

first use of the smart card is stored, and a secret memory area (*M*g) where data on said application are stored in protected fashion.

S:\Producer\jek\RICHTER - RICH3001\appendix of claims wpd

APPENDIX OF MARKED UP VERSION OF CLAIMS

1(Amended). A method for putting into operation a processor smart card for a network for communication, [preferably] for example a GSM network, wherein the card user must identify himself with respect to the processor smart card (SIM) by a personal identification number, [characterized in that] comprising the steps:

- for execution control of the first use, the processor smart card is first provided by the card manufacturer or card personalizer with an additional application, preferably using the SIM Application Toolkit, which prevents its use in the network, instead allowing only local use by means of a card reader or card terminal, preferably a mobile phone device, and

- upon the first use of the processor smart card, the application outputs without a further check of a secret number a display signal for the first use and a request for confirmation, and

- after receiving a confirmation signal the additional application is deactivated or its execution so changed that upon the next use of the card a display signal is outputted to indicate that the card has already been put into operation and the use of the processor smart card in the network is enabled.

2(Amended). [A] The method according to claim 1, [characterized in that] wherein a personal identification number previously defined, preferably by the card manufacturer or card personalizer, must be inputted for activating the additional application.

3(Amended). [A] The method according to claim 1 or 2, [characterized in that] wherein the entry of a personal identification number (PIN) and/or a secret number (PUK) for changing or unblocking the personal identification number (PIN) is requested after the first use of the card and prior to the deactivation or change of state of the additional application.

4(Amended). [A] The method according to any of claims 1 [to 3, characterized in that] or 2, wherein some or all personal identification numbers on the card were already personalized on the processor smart card by the card manufacturer and said numbers are indicated upon the first use for later use on the card reader or card terminal, preferably a mobile phone device.

5(Amended). [A] The method according to [any of claims 1 to 4, characterized in that] claim 1, wherein some or all personal identification numbers on the card are set by a random-number generator built into the card and said numbers are indicated during the first use on the card reader or card terminal, preferably a mobile phone device.

6(Amended). [A] The method according to [any of claims 1 to 5, characterized in that] claim 1, wherein some or all personal identification numbers are combined for transmission to the network, preferably in encrypted form via a data channel, and sent immediately or at a later time to a central place at the network operator or network service provider.

7(Amended). [A] The method according to [any of claims 1 to 6, characterized in that] claim 1, wherein the secret numbers to be defined at the first putting into operation are used not for the purpose of protecting the network application but for protecting an additional application, preferably a SIM Application Toolkit application, on the SIM card.

8(Amended). [A] The method according to [any of claims 1 to 7, characterized in that] claim 1, wherein information, on the first use of the processor smart card and on the personal identification numbers is outputted or inputted via the hearing or speaking devices of the card reader, the card terminal or preferably the mobile phone device.

9(Amended). A smart card [having] comprising a microprocessor (μP), a memory area (M) and an interface (*S*) each connected with the microprocessor (μP), [characterized by] and further comprising a memory area (*A*) where an application for the execution control of the first use of the smart card is stored, and a secret memory area (*M*g) where data on said application are stored in protected fashion.

S:\Producer\jek\RICHTER - RICH3001\appendix of marked up version of claims.wpd

Device for protecting the first use of a processor smart card

This invention relates to a method for protection from attacks on a processor smart card or from its unauthorized use in a network for communication, preferably a GSM network, according to the preamble of claim 1, and to a corresponding smart card according to the preamble of claim 9.

In GSM systems it is known that for using the smart card (Subscriber Identity Module SIM) the card user must first identify himself as a legitimate user by means of a Personal Identification Number (PIN). To avoid abuse at this point it is known to transmit the PIN to the card user by having PIN/PUK letters produced by the card manufacturer or card personalizer and handing over said PIN/PUK letters to the card user.

Another, system-relevant security measure is the sealing of the PIN/PUK letter by the card manufacturer or card personalizer. The intactness of the seal on the PIN/PUK letter indicates to the card user that the secret numbers applied to the PIN/PUK letter by the card manufacturer cannot be known to any other card user. Since the secret numbers on the PIN/PUK letter were chosen randomly by the card manufacturer or card personalizer and are stored only in the secret memory of the SIM card, the card user can assume that by opening the PIN/PUK letter only he himself acquires knowledge of the secret numbers.

To avoid abuse upon PIN entry, it is known for PIN entry to provide an error counter that temporarily prevents further use of the card when a permissible number of abortive attempts is exceeded. To protect from unnecessary blocking of a card by inadvertent false entry of the PIN, it is known to provide on the card a Personal Unblocking Key (PUK) which can be used to define a new PIN and which reenables the card for use in the network. To avoid abuse upon PUK entry, it is known to provide an error counter which definitively prevents further use of the card when a permissible number of abortive attempts is exceeded.

In the known prior art, the card user is given the possibility of replacing the PIN defined by the card manufacturer or card personalizer by a self-chosen value. The value of the PUK cannot be changed by the card user. To be able to inform the

card user of the PUK if the PIN/PUK letter is lost or inaccessible but the PIN inadvertently blocked, it is known to store the PUK additionally in a data base centrally with the network operator for all issued cards as a special service in some GSM networks. At the card user's request and after a check of the card user's identity, the PUK is transmitted to the card user for enabling the PIN.

Such a system also involves the danger that, by unauthorized opening of the PIN/PUK letter and for example by reprinting of the PIN/PUK letter or by manipulation of the PIN/PUK letter seal, the legitimate card user believes that he is the first user of the card although an illegitimate card user has already put the card into operation temporarily at the expense of the legitimate card user.

It is therefore the problem of the invention to provide a safe method for protection from unnoticed opening of PIN/PUK letters by which the first user of the card is notified of the first use of the card, as well as a corresponding smart card.

This problem is solved starting out from the features of the preambles of claim 1 and 9 by the respective characterizing features. Advantageous embodiments of the invention are stated in the dependent claims.

The invention relates to a method for checking and displaying the first use of a processor smart card by means of an additional application on the processor smart card itself which controls or at least substantially influences all steps necessary for a safe check.

An advantageous embodiment of the invention shows the use of the application to let the card user define secret keys required for authentication of the card user with respect to the card, or to transmit said keys to the card user, whereby the card remains transport-protected on the way between card manufacturer, card issuer and card user.

Another advantageous use of the invention is the supplementing or replacement of elaborate and sometimes cost-intensive methods for transport protection of processor smart cards between card manufacturer and card user, for example PIN/PUK letters, by the additional application in the processor smart card which supplements or substantially performs the function of a PIN/PUK letter.

According to another advantageous embodiment, the invention can also be used as a component of a system executed in essential parts in the processor smart card itself for individual allocation and personalization of secret keys which are to be made accessible not only to the card user but also to the card issuer, e.g. a mobile phone network operator or network service provider.

Another advantageous embodiment of the invention provides that when the secret keys are defined by the card user himself, said secret keys are asked for several times by the card user in order to avoid inadvertent false entry.

Alternatively or additionally, after the secret numbers have been defined by the card user or by the card itself a corresponding network component can be sent a message after which the first use of the card in the network is communicated or the value of the secret number transmitted.

According to another advantageous embodiment of the invention, when the card is first put into operation the secret numbers are additionally or alternatively inputted or outputted via the speaking or hearing apparatus of the mobile phone device, which can in particular facilitate and better protect the transmission or definition of secret keys to or by visually handicapped card users.

Fig. 1 shows an example of smart card *SIM* having interface *S* for data exchange with a mobile phone and microprocessor μP connected with application *A* and memory *M*, *Mg*. Application *A* can be formed substantially as a SIM Application Toolkit application and has been incorporated into the card by the card manufacturer or card personalizer. The memory is divided into usual memory area *M* where data can be read and written, and secret memory area *Mg* where at least the information about the first use of the smart card is stored. When the card is put into operation by a card user via interface *S*, the application checks by accessing secret memory *Mg* whether this is the first use of the card.

Upon the first use of the card, the card user is informed by application *A* and asked to confirm the putting into operation of the card. Upon positive confirmation by the card user, the application changes the information about first use in secret memory *Mg*, thereby changing its behavior when the card is put into operation again later.

Patent claims

1. A method for putting into operation a processor smart card for a network for communication, preferably a GSM network, wherein the card user must identify himself with respect to the processor smart card (SIM) by a personal identification number, characterized in that
   - for execution control of the first use, the processor smart card is first provided by the card manufacturer or card personalizer with an additional application, preferably using the SIM Application Toolkit, which prevents its use in the network, instead allowing only local use by means of a card reader or card terminal, preferably a mobile phone device, and
   - upon the first use of the processor smart card, the application outputs without a further check of a secret number a display signal for the first use and a request for confirmation, and
   - after receiving a confirmation signal the additional application is deactivated or its execution so changed that upon the next use of the card a display signal is outputted to indicate that the card has already been put into operation and the use of the processor smart card in the network is enabled.
2. A method according to claim 1, characterized in that a personal identification number previously defined, preferably by the card manufacturer or card personalizer, must be inputted for activating the additional application.
3. A method according to claim 1 or 2, characterized in that the entry of a personal identification number (PIN) and/or a secret number (PUK) for changing or unblocking the personal identification number (PIN) is requested after the first use of the card and prior to the deactivation or change of state of the additional application.
4. A method according to any of claims 1 to 3, characterized in that some or all personal identification numbers on the card were already personalized on the processor smart card by the card manufacturer and said numbers are indicated

upon the first use for later use on the card reader or card terminal, preferably a mobile phone device.

5. A method according to any of claims 1 to 4, characterized in that some or all personal identification numbers on the card are set by a random-number generator built into the card and said numbers are indicated during the first use on the card reader or card terminal, preferably a mobile phone device.

6. A method according to any of claims 1 to 5, characterized in that some or all personal identification numbers are combined for transmission to the network, preferably in encrypted form via a data channel, and sent immediately or at a later time to a central place at the network operator or network service provider.

7. A method according to any of claims 1 to 6, characterized in that the secret numbers to be defined at the first putting into operation are used not for the purpose of protecting the network application but for protecting an additional application, preferably a SIM Application Toolkit application, on the SIM card.

8. A method according to any of claims 1 to 7, characterized in that information on the first use of the processor smart card and on the personal identification numbers is outputted or inputted via the hearing or speaking devices of the card reader, the card terminal or preferably the mobile phone device.

9. A smart card having a microprocessor (μP), a memory area (M) and an interface (S) each connected with the microprocessor (μP), characterized by a memory area (A) where an application for the execution control of the first use of the smart card is stored, and a secret memory area (Mg) where data on said application are stored in protected fashion.

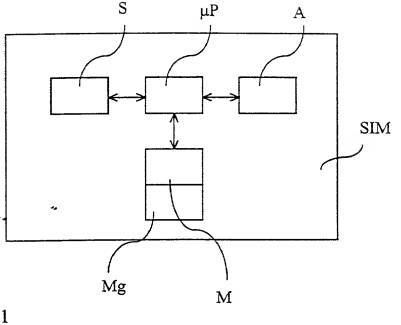

Fig. 1

ATTORNEY/DOCKET NO **RICH3001/JEK**

DECLARATION FOR PATENT APPLICATION AND APPOINTMENT OF ATTORNEY

As a below named inventor, I hereby declare that my residence, post office address and citizenship are as stated below next to my name; I believe that I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention (Design, if applicable) entitled: **DEVICE FOR PROTECTING THE INITIAL UTILIZATION OF A PROCESSOR/CHIP CARD** the specification of which (check one):

☐ is attached hereto, or ☒ was filed on: **09 May 2000** as U.S. Application Number or PCT International Application Number: **(PCT/EP00/04141) 09/926,460** and (if applicable) was amended on:

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment(s) referred to above. I acknowledge the duty to disclose information which is material to patentability as defined in *Title 37, Code of Federal Regulations, §1 56.* I hereby claim foreign priority benefits under *Title 35, United States Code §119* of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed.

PRIOR FOREIGN APPLICATION(S)			PRIORITY CLAIMED	
Number	Country	Day/Month/Year Filed	Yes	No
199 21 524.3	Germany	10 May 1999	X	

☐ Additional Priority Application(s) Listed on Following Page(s)

I HEREBY CLAIM THE BENEFIT UNDER TITLE 35 U.S. CODE §119(E) OF ANY U.S. PROVISIONAL APPLICATIONS LISTED BELOW.

Application Number	Day/Month/Year Filed

☐ Additional Provisional Application(s) Listed on Following Page(s)

I hereby claim the benefit under *Title 35, United States Code, §120* of any United States application(s) or PCT international application(s) designating The United States of America listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in that/those prior application(s) in the manner provided by the first paragraph of *Title 35, United States Code, §112*, I acknowledge the duty to disclose information which is material to patentability as defined in *Title 37, Code of Federal Regulations, §1.56* which became available between the filing date of the prior application(s) and the national or PCT international filing date of this application:

Application Number	Filing Date	Status - Patented, Pending or Abandoned

☐ Additional US/PCT Priority Application(s) listed on Following Page(s)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under *section 1001 of title 18 of the United States Code* and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: I (We) hereby appoint as my (our) attorneys, with full powers of substitution and revocation, to prosecute this application and transact all business in the Patent and Trademark Office connected therewith: J. Ernest Kenney, Reg. No. 19,179; Eugene Mar, Reg. No. 25,893; Richard E. Fichter, Reg. No. 26,382; Thomas J. Moore, Reg. No. 28,974, Joseph DeBenedictis, Reg. No. 38,502, Benjamin E. Urcia, Reg. No. 33,805; and

I(we) authorize my(our) attorneys to accept and follow instructions from **Klunker Schmitt-Nilson Hirsch** regarding any matter related to the preparation, examination, grant and maintenance of this application, any continuation, continuation-in-part or divisional based thereon, and any patent resulting therefrom, until I(we) or my(our) assigns withdraw this authorization in writing.

Send correspondence to: Customer 23364

BACON & THOMAS, PLLC
625 Slaters Lane - 4th Floor
Alexandria, VA 22314-1176

Telephone Calls to: **J. Ernest Kenney** **(703) 683-0500**

FULL NAME OF FIRST OR SOLE INVENTOR	CITIZENSHIP
Oliver RICHTER	**Germany**
RESIDENCE ADDRESS ~~Ottilienstrasse 52a, 81827 München~~, Germany Max-Beckmann-Str. 30, 81735 München DE	POST OFFICE ADDRESS IS THE SAME AS RESIDENCE ADDRESS UNLESS OTHERWISE SHOWN BELOW
DATE 27.12.2001	SIGNATURE X Oliver Richter

☐ *See following page(s) for additional joint inventors.*